

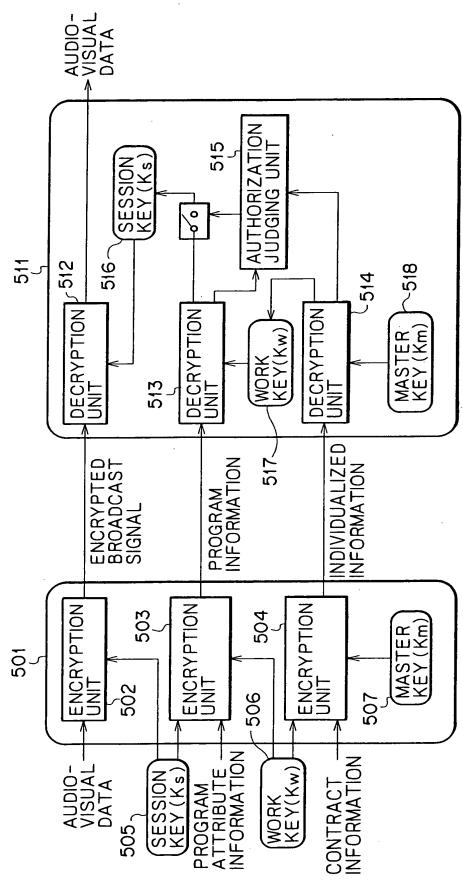
APPROVED	O.G. FIG.		
BY	CLASS SUBCLASS		
DRAFTSMAN			

F 1 G 4

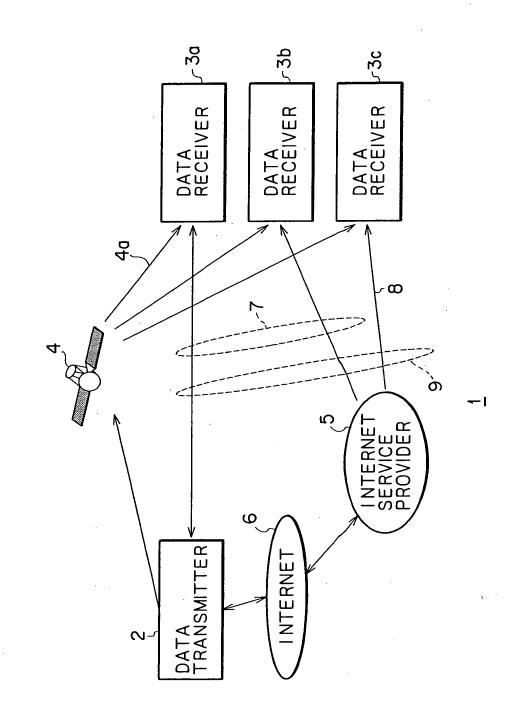
413 د	SCRAMBLE ADAPTATION CYCLIC ADAPTATION PAYLOAD CONTROL COUNTER FIELD (INFORMATION)		
	ADAPTATION FIELD	4bits 8×Nbits	
	CYCL IC COUNTER	4bits	
	ADAPTATION FIELD CONTROL	2bits	188bytes
411 412	SCRAMBLE CONTROL	13bits 2bits	188
4 2	PID	13bits	
	TRANSPORT PACKET PRIORITY	1bit	
	UNIT START INDICATION	16i t	
	SYNCHRO- ERROR UNIT START TRANSPORT NIZING INDICATION INDICATION PRIORITY	1bit	
	SYNCHRO- NIZING BYTE	8bits	

APPROVED	O.G. FIG.		
BY	CLASS	SUBCLASS	
ORAFTSMAN			

F | G.5

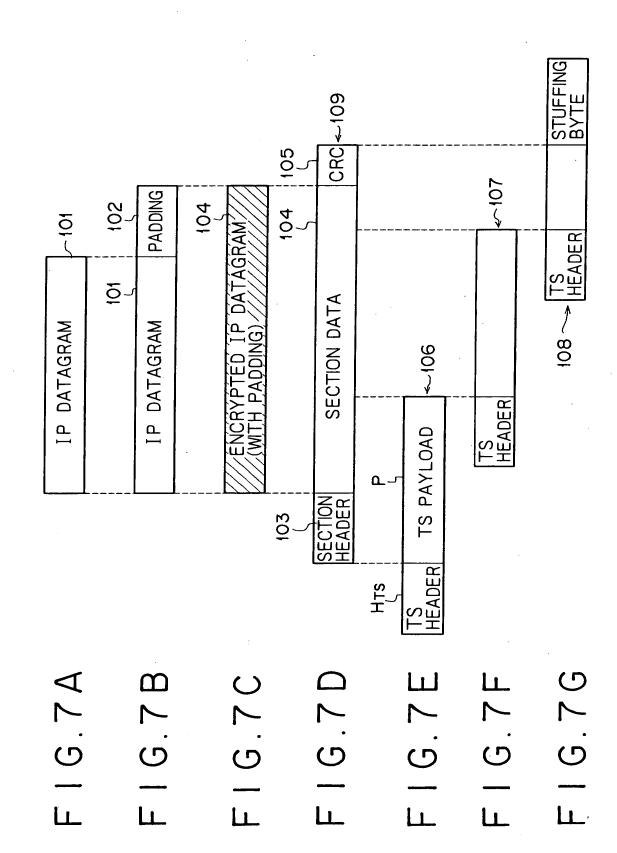


F | G.6



contain the contains

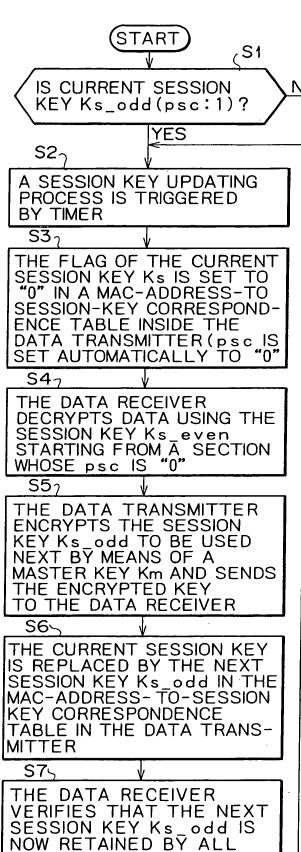
APPROVED	O.G. FIG.		
BY	CLASS	SUBCLASS	
DPAFTSMAN			



APPROVED	O.G. FIG.		
вч	CLASS	SUBCLASS	
DRAFTSMAN			

➤ DATA 3 CA MANAGING UNIT DECRYPTION UNIT 33 DECRYPTION UNIT MASTER KEY (Km) SESSION KEY (Ks) 35 RESTRICTIVE DATA TRANSMISSION CONTROL ENCRYPTED SESSION KEY Ks **NFORMATION** ENCRYPTED DATA CA MANAGING UNIT ENCRYPTION UNIT ENCRYPTION UNIT 22 25 **(23** 2 MASTER KEY (Km) 7٦٦ DATA -SESSION KEY (Ks) 24

PPROVED O.G. FIG.
BY CLASS SUBCLASS



TARGET DATA RECEIVERS

F 1 G.9 NO **CS8** A SESSION KEY UPDATING PROCESS IS TRIGGERED BY TIMER $\langle S9 \rangle$ THE FLAG OF THE CURRENT SESSION KEY Ks IS SET TO "1" IN A MAC-ADDRESS-TO SESSION-KEY CORRESPOND-ENCE TABLE INSIDE THE DATA TRANSMITTER (psc IS SET AUTOMATICALLY TO < S10 THE DATA RECEIVER DECRYPTS DATA USING THE SESSION KEY Ks_odd STARTING FROM A SECTION WHOSE psc IS "1" WHOSE psc IS < S11 THE DATA TRANSMITTER ENCRYPTS THE SESSION KEY Ks_even TO BE USED NEXT BY MEANS OF THE MASTER KEY Km AND SENDS THE ENCRYPTED KEY TO THE DATA RECEIVER ∠S12

THE CURRENT SESSION KEY IS REPLACED BY THE NEXT SESSION KEY Ks_even IN THE MAC-ADDRESS-TO-SESSION KEY CORRESPONDENCE TABLE IN THE DATA TRANS-MITTER

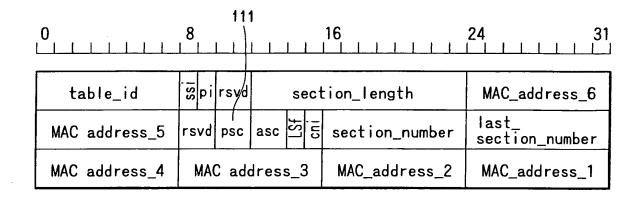
THE DATA RECEIVER VERIFIES THAT THE NEXT SESSION KEY Ks_even IS NOW RETAINED BY ALL TARGET DATA RECEIVERS

c S13

COUNTY OF THE PERSON OF THE PE

APFAOVED O.G. FIG.
BY CLASS SUBCLASS
DRAFTSMAN

F I G.10



ssi : section_syntax_indicator

pi : private_indicator

rsvd: reserved

psc : payload_scramble_indicator
asc : address_scramble_indicator

LSf : LLC_SNAP_flag

cni : current_next_indicator

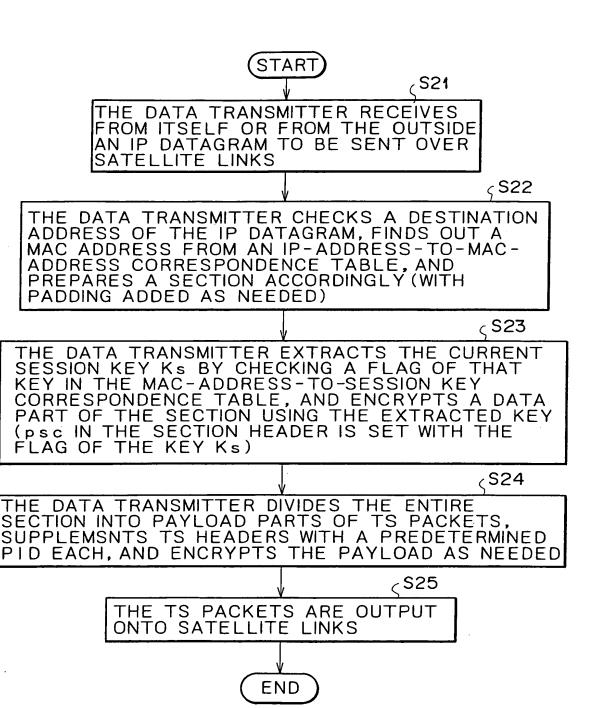
F I G.11

112

MAC ADDRESS	Ks_even	Ks_odd	Ks FLAG
08:00:46:01:07:24	0×C08F25	0×90B3AF	0
08:00:45:01:07:09	0×26D261	0×BA023C	1
01:00:5e:16:0:0	0×461E67	0×DC1A22	0

APTROVED O.G. FIG.
BY CLASS SUBCLASS
CRAFTSMAN

F I G.12



SS SUBCLASS

F I G.13

IP ADDRESS	bitmask	MAC address
133. 11. 9. 39	255. 255. 255. 225	08:00:46:01:07:24
133. 11. 20. 0	255. 255. 255. 0	08:00:46:01:07:09
226. 0. 0. 0	255. 255. 255. 224	01:00:5e:16:0:0

F I G.15

MAC ADDRESS	Ks_even	Ks_odd
08:00:46:01:07:24	0×C08F25	0×90B3AF
01:00:5e:16:0:0	0×461E67	0×DC1A22

F I G.16

113

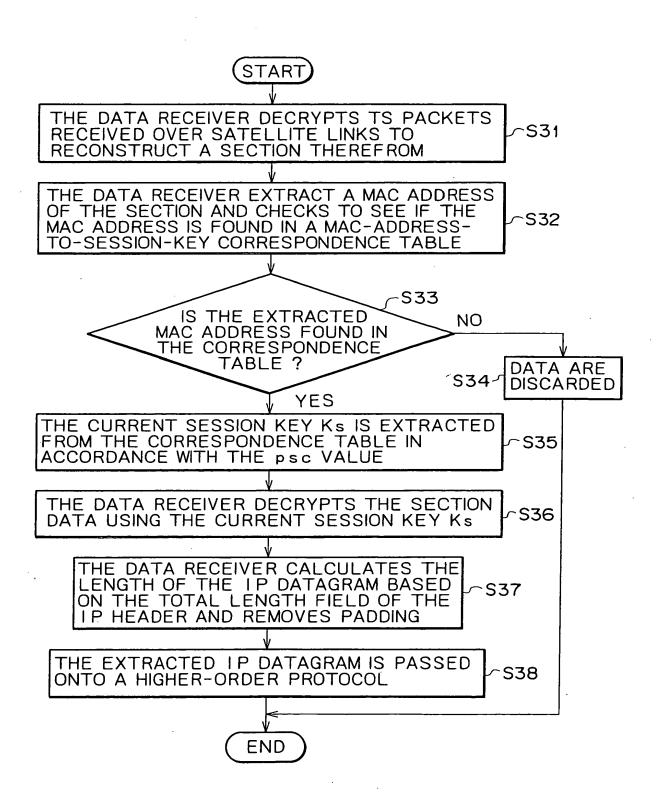
VERS	HLEN	SERVIE TYPE	Т	OTAL LENGTH
	IDENTIFICAION		FLAGS	FRAGMENT OFFSET
TIME T	O LIVE	PROTOCOL	H	EADER CHECKSUM
	SOURCE IP ADDRESS			
DESTINATION IP ADDRESS				
	IP OPTIONS (IF ANY) PADDING			PADDING
	DATA			

DRAFTSMAN

CLASS

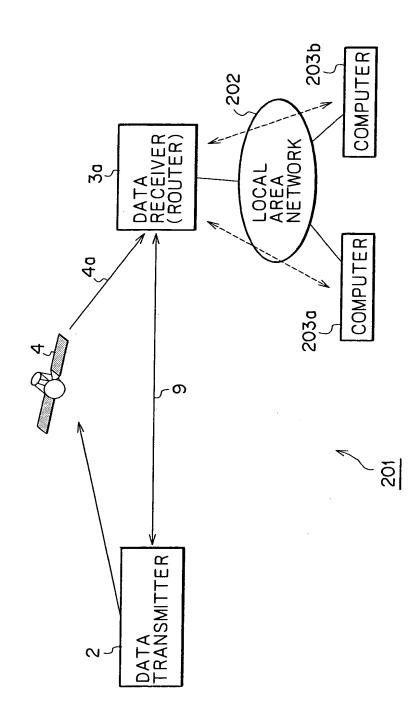
SUBCLASS

F I G.14



APPROVED	O.G. FIG.		
BY	CLASS	SUBCLASS	
DRAFTSMAN			

F I G.17



APPROVED O.G. FIG.
BY CLASS SUBCLASS
DRAFTSMAN

